⑲ 日本国特許庁（JP）　　⑪ 特許出願公開

⑫ 公開特許公報（A）　　昭60—26387

⑤Int. Cl.⁴	識別記号	庁内整理番号
G 09 C 1/00		7368—5B
H 04 L 9/02		7240—5K

⑬公開　昭和60年(1985) 2月9日

発明の数　1
審査請求　有

（全 7 頁）

⑭デイジタル署名方式

⑳特　　願　昭58—134853
㉒出　　願　昭58(1983) 7月22日
㉑発 明 者　小山謙二　武蔵野市緑町3丁目9番11号日本電信電話公社武蔵野電気通信研究所内
㉑出 願 人　日本電信電話公社
㉔代 理 人　弁理士　草野卓

明　細　書

1. 発明の名称

デイジタル署名方式

2. 特許請求の範囲

(1) デイジタル情報の通信または蓄積を行うシステムにおいて、送信側に平文メッセージをデータ圧縮して認証子を生成する手段と、この認証子を公開暗号方法における秘密鍵を用いて暗号処理して認証メッセージを生成する手段と、前記平文メッセージと前記認証メッセージを送信または蓄積する手段を備え、受信側に送られてきたまたは読み出された平文メッセージを送信側と同一手法によりデータ圧縮して認証子を生成する手段と、送られてきたまたは読み出された認証メッセージから前記公開暗号方法における公開鍵を用いて暗号処理の逆変換をして元の認証子を復元する手段と、これらの認証子を照合する手段を備え、前記送信側よりの平文メッセージ及び認証メッセージから送信者の身元の確認と通信中での改ざんの有無の確認をして認証することを特徴とするデイジタル署名方式。

3. 発明の詳細な説明

発明の属する分野の説明

この発明は、送信者より送られてきたデイジタル情報の平文メッセージに対し、受信者が送信者の身元の確認と通信中での改ざんの有無の確認をして認証する方式、デイジタル署名方式に関する。

従来技術とその問題点

従来の署名は紙の上に書かれた個人特有の筆跡によりその文書の内容と筆者が正しいものであることの認証が行われてきた。しかしこの従来の署名をデータ通信にそのまま適用しようとすると、認証機能を果すことができない。従つて例えばデイジタル情報を用いて買物の注文を行う場合に、注文をしないのに注文をしたことにされたり、注文の内容を変更されたりすることが容易に行われる可能性がある、また著者が文章を記憶装置にデイジタル情報としてファイルし、読者がそのファイルを読出した時に、その読出した内容の著者が間違いないものと確認できることが望まれる。デイジタル情報に対しても従来の署名と同様の機能を果すことができることが要請されており、この解決策がデイジタル署名と呼ばれるものである。6

ディジタル署名においては、安全性の観点から、次の2条件(A)と(B)を満たすことが必要である。

(A) 署名付きメッセージが第三者によつて偽造できない。

(B) 署名付きメッセージが受信者によつて偽造できない。

従来のディジタル署名法を、①ディジタル署名に用いる暗号法と、②署名付きメッセージの検査法の観点から分類し、その特徴を以下に述べる。

① 暗号法による分類

ディジタル署名を行うために用いられる暗号として、(a)慣用暗号と(b)公開鍵暗号がある。

(a) 慣用暗号

慣用暗号とは、暗号化鍵と復号化鍵が同一でそれぞれ秘密にしておく暗号である。現在の代表的な慣用暗号としてDES(Data Encryption Standard)がある。慣用暗号によるディジタル署名では、送信者と受信者のみで共有している秘密の鍵で署名付きメッセージを生成し、これを送信し、受信者はその受信メッセージを前記秘密の鍵で解読するものであり、前記条件(A)は満たされるが、条件(B)は満たされていない欠点がある。

(b) 公開鍵暗号

公開鍵暗号とは、一対の暗号化鍵と復号化鍵が異なり、暗号化鍵は公開し、復号化鍵のみを秘密にしておく暗号である。現在の代表的な公開鍵暗号としてRSA法〔R.L.Rivest, A.Shamir and A.Adleman "Amethod for obtaining digital signatures and public-key cryptosystem", CACM, 21, №2, pp120−126, 1978〕と、R法〔M.O.Rabin "Digitalized signatures and public-key functions as intractable as factorization," Tech.Rep.MIT/LCS/TR MIT Lab.Comput. Sci., 1979〕がある。公開鍵暗号によるディジタル署名では、送信者のみが秘密に保持している鍵(復号化鍵)を用いて暗号処理(復号化)を行つて署名付きメッセージを生成し、受信者はそのメッセージを公開鍵で復号(暗号化)処理をするものであり、前記条件(A)と(B)は満たされる。公開鍵暗号によるディジタル署名は、調停者(秘密性を高くするために信頼される調停者を介して送ることがある)がいなくても前記の条件(A),(B)を満たすので、"真の署名",または、"直接署名"と呼ばれている。

RSA法の特徴は、すべてのメッセージに対して署名が可能であるが、暗号化と復号化の計算量が多いことが欠点である。R法の特徴は、暗号化の計算量が少ないが、すべてのメッセージに対して署名が可能とは限らないことが欠点である。

② 検査法による分類

ディジタル署名の検査法として、(a)メッセージ復元法と(b)認証子法がある。

(a) メッセージ復元法

メッセージ復元法では、まず、送信者が平文メッセージに暗号処理をして署名付きメッセージの一種である認証メッセージに変換し、受信者に送る。次に、受信者は送られてきた認証メッセージに暗号処理の逆変換を施して元の平文メッセージを復元する。復元された平文メッセージが意味のあるものならば、(例えば、日本語として意味をなすものならば)受信者はメッセージの送信者と内容が正しいと認証する。

この方式は暗号を用い、暗号化と復号化による双方向の操作で実現している。しかし、復元された平文メッセージの意味理解を、人間が介在しないので機械的(自動的)に行うのは容易でないという欠点がある。

(b) 認証子法

認証子法は検証とも呼ばれている。認証子法では、まず、送信者が平文メッセージに暗号処理(スクランブル)をして、署名付きメッセージの一種である認証子に変換し、この認証子を生のままの平文メッセージとともに受信者に送る。受信者は送られてきた生のままの平文メッセージに同様の暗号処理(スクランブル)をして新たに認証子を生成し、送られてきた認証子と照合する。もし、一致したならば、受信者はメッセージの送信者と内容が正しいと認証する。

この方式は秘密の鍵で一方向のスクランブルを行うことによつて実現しており、必ずしも逆変換

が保証されている暗号を用いなくともよい。この方式は、送信者と受信者で共通の秘密鍵を保持することが必要なので、鍵配送が困難なことと安全性の条件(B)を満たさないという欠点がある。

また認証子法には安全性を損なわない範囲で平文メッセージに、ハッシング法によりデータ圧縮を行い、小さなサイズの認証子を生成する効率的な検証方式も提案され、効率と安全性を満たす手法として、認証子の生成にDESをCBC(Cipher Block Chaining)モードで用い、32ビットの認証子を生成する手法がANSI(米国規格協会)とISO(国際標準化機構)で推奨されている。しかし、このデータ圧縮法は、慣用暗号を用いているので、鍵配送が困難なことと安全性の条件(B)を満たさないことは変わりない。さらに、データ圧縮の計算量が多いと云う欠点もある。

発明の目的

この発明は従来のデイジタル署名の方式の問題点を解決させ、通信または記憶における認証を前記条件(A),(B)を満し、機械的に行うことができ、かつ、鍵管理を容易にし、認証処理の高速化を図ることを目的としたものである。

発明の概要

この発明では、例えばRabinの公開鍵暗号法(R法)の暗号化関数によつてメッセージをデータ圧縮して認証子を生成し、この認証子を新たなメッセージとして、RSA法によるメッセージ復元法を適用する。以下に、その手順を示す。

(イ) 送信者は平文メッセージMを例えば512ビット毎のブロックに分割する。

$M=<M1, M2, \cdots\cdots, Mm>$

各ブロックMi($1 \leq i \leq m$)に対し、R法の暗号化関数をCBCモードで適用し、認証子Tを生成する。

$T=f(M, b, n)$

ただし、bとnは送信者及び受信者を初め第三者も知つている公開鍵である。fは具体的には

$C1=M1(M1+b) \pmod n$

$N2=M2 \oplus C1$

$C2=N2(N2+b) \pmod n$

$N3=M3 \oplus C2$

$C3=N3(N3+b) \pmod n$

.....

$Nm=Mm \oplus Cm-1$

$Cm=Nm(Nm+b) \pmod n$

$T=Cm \quad (1)$

となる。ただし、bとnのサイズは512ビットであり、⊕は排他的論理和を表す。

(ロ) 送信者はT(512ビット)に対し、自分しか知らない秘密鍵dと全員が知つている公開鍵nを用いてRSA法の復号化処理gを行い、認証メッセージVを生成する。

$V=g(T, d, n)=T^d \pmod n \quad (2)$

ただし、式(1)と式(2)のnは同じ値である。

平文メッセージMと認証メッセージVを受信者に送る。

(ハ) 受信者は送られてきた平文メッセージMに対し、(イ)と同様に公開鍵bとnを用いて認証子Tを生成する。

$T=f(M, b, n)$

もし、平文メッセージMが途中でM'に改ざんされている場合はこの(ハ)の処理により認証子として

$T'=f(M', b, n)$

が得られる。

(ニ) 受信者は、さらに、送られてきた認証メッセージVに対し、公開鍵eとnを用いてRSA法の暗号化処理g^{-1}を行い、認証子Tを復元する。

$T=g^{-1}(V, e, n)=V^e \pmod n \quad (3a)$

ただし、eとdは、$V^{ed} \equiv V \pmod n$を満たす鍵のペアである。もし、認証メッセージVが途中でV'に改ざんされるか、第三者が最初からV'を偽造した場合は、(ニ)の処理により認証子として

$T''=g^{-1}(V', e, n)=V'^e \pmod n \quad (3b)$

が得られる。ただし、式(1)と式(3a),(3b)のnは同じ値である。

(ホ) 受信者は(ハ)で得られた認証子Tまたは、T'と(ニ)で得られた認証子Tまたは、T''とを比較判定し、もし、一致することを確認したならば、メッセージMが改ざんされていないことと送信者の身元が正しいことを認証する。

即ち、MとVが改ざんされていなければ、(ｲ)で得られたTと(ﾆ)で得られたTは等しい。もし、Mだけが改ざんされていれば、(ｲ)で得られたT'と(ﾆ)で得られたTは等しくない。もし、Vだけが改ざんされていれば、(ｲ)で得られたTと(ﾆ)で得られたT"は等しくない。もし、MとVの両方が改ざんされていれば、(ｲ)で得られたT'と(ﾆ)で得られたT"は等しくない。

以上の手順の流れを第1図に示す。

実施例の説明

第2図はこの発明のデイジタル署名方式を実現する認証メッセージ送信装置1と認証メッセージ受信装置2の構成図である。線3で示すように通信の途中で第三者によるメッセージの改ざんのない場合と、線4で示すように通信の途中で第三者が改ざん装置5を用いて改ざんする場合とを説明する。

送信者は認証メッセージ送信装置1に、メッセージMと秘密鍵dと公開鍵bとnを入力してVを生成し、MとVを送信する。もし、通信の途中で第三者の改ざんがなければ、受信者は受信したM及びVと、公開鍵b，n，eとを認証メッセージ受信装置2に入力して、改ざんがなかつたことを示す出力結果を得る。通信の途中で第三者がMとVをそれぞれM'とV'に改ざんしたとする。受信者は受信したM'及びV'と公開鍵b，n，eとを認証メッセージ受信装置2に入力して、改ざんがあつたことを示す出力結果を得る。このように、認証メッセージ受信装置2の出力結果によつて、受信者は本当の送信者が送つたメッセージがまちがいなく届いたかどうかを認証する

第2図における認証メッセージ送信装置1の詳細を第3図に示し、認証メッセージ受信装置2の詳細を第4図に示す。

第3図の認証メッセージ送信装置の詳細な動作を説明する。データ読み込み回路11に平文メッセージMが入力されると512ビット毎のm個のブロック<M1，M2，…… Mm>に分割されてデータ格納メモリ14の領域14bに格納される。さらに、データ読み込み回路11に公開鍵b，nと秘密鍵dが入力されて領域14a，14eに格納される。これらを読出してブロック化されたメッセージ<M1，M2，……Mm>と公開鍵b，nをもとに、式(1)の関数fをデータ圧縮器12で実行し、中間変数Ci，Nj（1＜i＜m，2＜j＜m）を求めてメモリ14の領域14cに格納しながら最終的な認証子Tを求め、データ格納メモリ14の領域14dに格納する。次に、このようにして得られた領域14dのTと領域14eの入力された公開鍵nと秘密鍵dをもとに、式(2)の関数gを乗演算器13で実行して認証メッセージVを求め、データ格納メモリ14の領域14fに格納する。最終的に領域14dの平文メッセージMと領域14fの認証メッセージVを読出してデータ送信回路15を介して受信者へ通信する。

第4図の認証メッセージ受信装置の詳細な動作を説明する。改ざんがなかつた場合と改ざんがあつた場合を区別するために、以下、改ざんがなかつた場合の記号名と並べて改ざんがあつた場合の記号名を()でくくつて表す。データ受信回路25に平文メッセージM(M')と認証メッセージV(V')が入力され、データ読み込み回路21に公開鍵b，n，eとが入力されると、まず、M(M')は512ビット毎のm個のブロック<M1，M2，……Mm>（<M1'，M2'，……Mm'>）に分割されてデータ格納メモリ24の領域24bに格納され、Vは領域24fに格納され、鍵bn及びenはそれぞれ領域24a及び24eにそれぞれ格納される。次に、ブロック化されたメッセージ<M1，M2，……Mm>（<M1'，M2'，……Mm'>）と公開鍵b，nをもとに、式(1)の関数fをデータ圧縮器22で実行し、中間変数Ci（Ci'），Nj(Nj')（1＜i＜m，2＜j＜m）を求めながらデータ格納メモリ24の領域24cに格納しながら最終的な認証子T(T')を求め、データ格納メモリ24の領域24dに格納する。さらに、認証メッセージV(V')と公開鍵nとeをもとに、式(3)の関数g^{-1}を乗演算器23で実行して、認証子T(T")を生成し、領域24gに格納する。最後に、領域24dのT(T')と領域24gのT(T")とを比較器26により照合して認証する。もし、一致したなら、送信者の身元が正しく、平文メッセージが途中で改ざんされていないこと

を示し、この平文メッセージMをデータ書込み回路27を介して出力する。

なお、上述においてデータ圧縮はR法の暗号化関数をCBCモードで行う場合に限らず、単なるデータ圧縮でもよい。また認証メッセージを生成するために用いる公開暗号方法はRSA法に限ることなく、他の方法でもよい。更にデイジタル伝送に対するデイジタル署名のみならず、デイジタル情報を蓄積し、これを読出す場合のデイジタル署名にもこの発明は適用できる。

効果の説明

以上述べたこの発明のデイジタル署名方式は次の長所をもつている。

① 秘密鍵の配送が不要なこと。

この発明の手法はすべて公開鍵暗号を基本としているので秘密鍵（前記例のｄ）は送信者のみが保持すればよいので鍵管理が容易である。

② データ圧縮が高速、かつ、安全に実現できること。

データ圧縮に前記例ではR法を用いたが、R法の暗号化関数はDESアルゴリズムよりも計算量が小さい。また、公開鍵暗号法を用いているため受信者と第三者が認証子をそのままにしてメッセージを改ざんすることは困難である。つまり偽造した平文メッセージと対応する偽造した認証メッセージを作ることは困難であり、安全性が保たれる。

③ メッセージ復元法を高速に実現できること。

メッセージ復元法の対象となるメッセージがデータ圧縮された1ブロック（512ビット）の認証子なので、この例ではRSA法の計算量は少なくなる。

④ メッセージ復元法での意味処理が不要なこと。

データ圧縮によつて復元された認証子とメッセージ復元法で復元された認証子とを機械的にシンタックス・レベルで照合できるから、意味処理は不要となり、人間が介在することなく、機械的（自動的）に認証できる。

⑤ 認証子法とメッセージ復元法との整合性が良い。

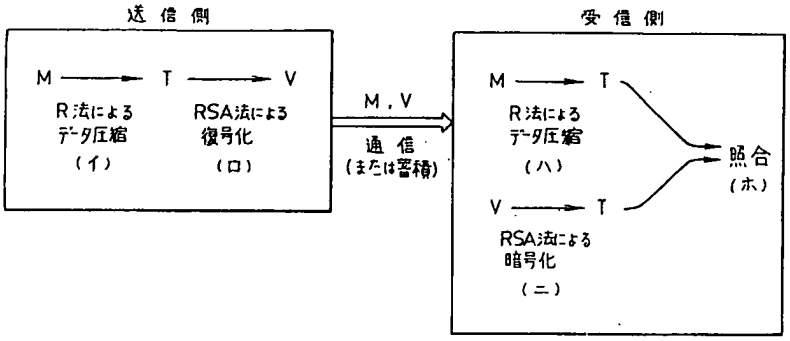
前記実施例ではR法とRSA法に同一の鍵ｎを用いているため同一のｎを法とした計算となるため、サイズの変換が不要であり、鍵生成も共通化できる。

4. 図面の簡単な説明

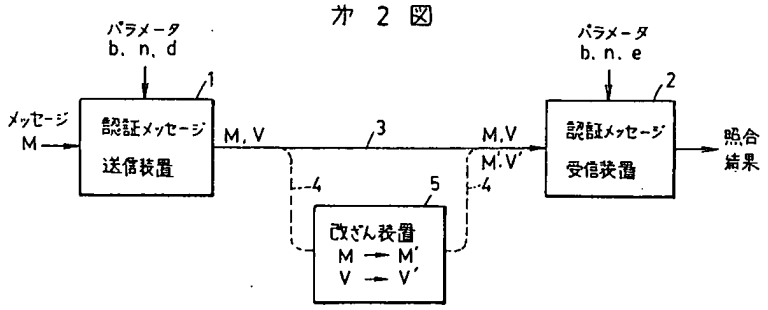
第1図はこの発明のデイジタル署名方式の情報の流れを示す図、第2図はこの発明のデイジタル署名方式の構成を示すブロック図、第3図は認証メッセージ送信装置の詳細例を示すブロック図、第4図は認証メッセージ受信装置の詳細例を示すブロック図である。

1…認証メッセージ送信装置、2…認証メッセージ受信装置、3…改ざんのない通信回線、4…改ざんのある通信回線、5…改ざん装置、11…データ読み込み回路、12…データ圧縮器、13…べき乗演算器、14…データ格納メモリ、15…データ送信回路、21…データ読み込み回路、22…データ圧縮器、23…べき乗演算器、24…データ格納メモリ、25…データ受信回路、26…比較器、27…データ書込み回路。

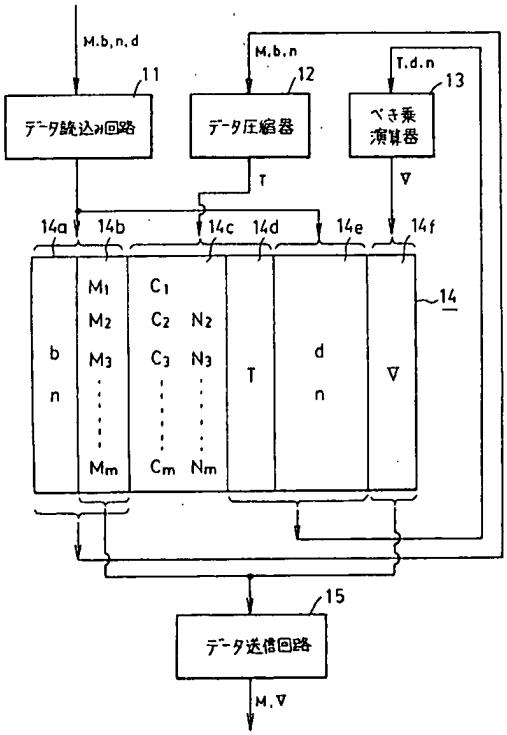
第 1 図


送信側
M
T
V
R法による
データ圧縮
(イ)
RSA法による
復号化
(ロ)
M, V
通信
(または蓄積)
受信側
M
T
R法による
データ圧縮
(ハ)
V
T
RSA法による
暗号化
(ニ)
照合
(ホ)

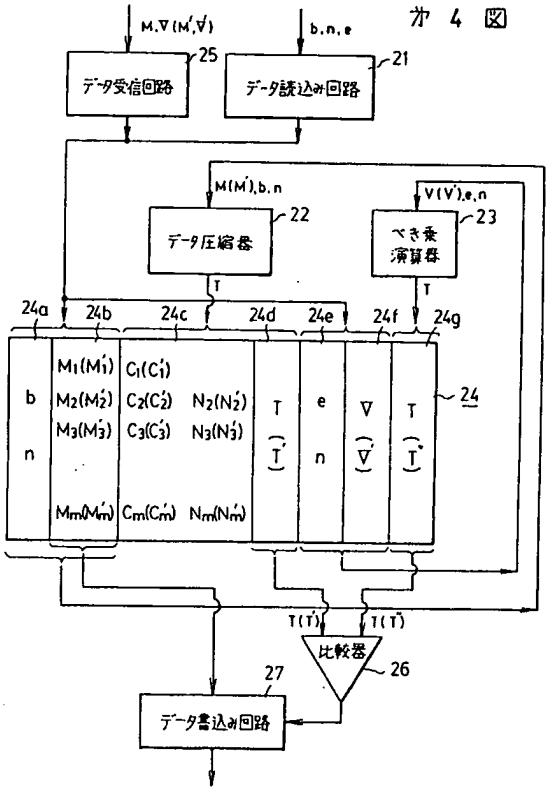
第 2 図


パラメータ
b, n, d
1
メッセージ
M
認証メッセージ
送信装置
M, V
3
M, V
M', V'
パラメータ
b, n, e
2
認証メッセージ
受信装置
照合
結果
4
5
4
改ざん装置
M → M'
V → V'

第 3 図


M,b,n,d
11
データ読込み回路
M,b,n
12
データ圧縮器
T,d,n
13
べき乗
演算器
T
∇
14a
14b
14c
14d
14e
14f
14
b
n
M1
M2
M3
Mm
C1
C2
N2
C3
N3
Cm
Nm
T
d
n
∇
15
データ送信回路
M, ∇

第 4 図


M,∇(M',∇')
b,n,e
25
データ受信回路
21
データ読込み回路
M(M'),b,n
V(V'),e,n
22
データ圧縮器
23
べき乗演算器
T
T
24a
24b
24c
24d
24e
24f
24g
b
n
M1(M'1)
M2(M'2)
M3(M'3)
Mm(M'm)
C1(C'1)
C2(C'2)
C3(C'3)
Cm(C'm)
N2(N'2)
N3(N'3)
Nm(N'm)
T
T'
e
n
∇
∇'
T
T'
24
T(T')
T(T')
比較器
26
27
データ書込み回路